KNOWLEDGE DECISIONS UNCERTAINTY RISK RESPONSIBILITY SUCCESS

MANAGING RISK

Training, facilitation, and mentoring activities to prepare NASA personnel to identify, manage, and effectively communicate risk.

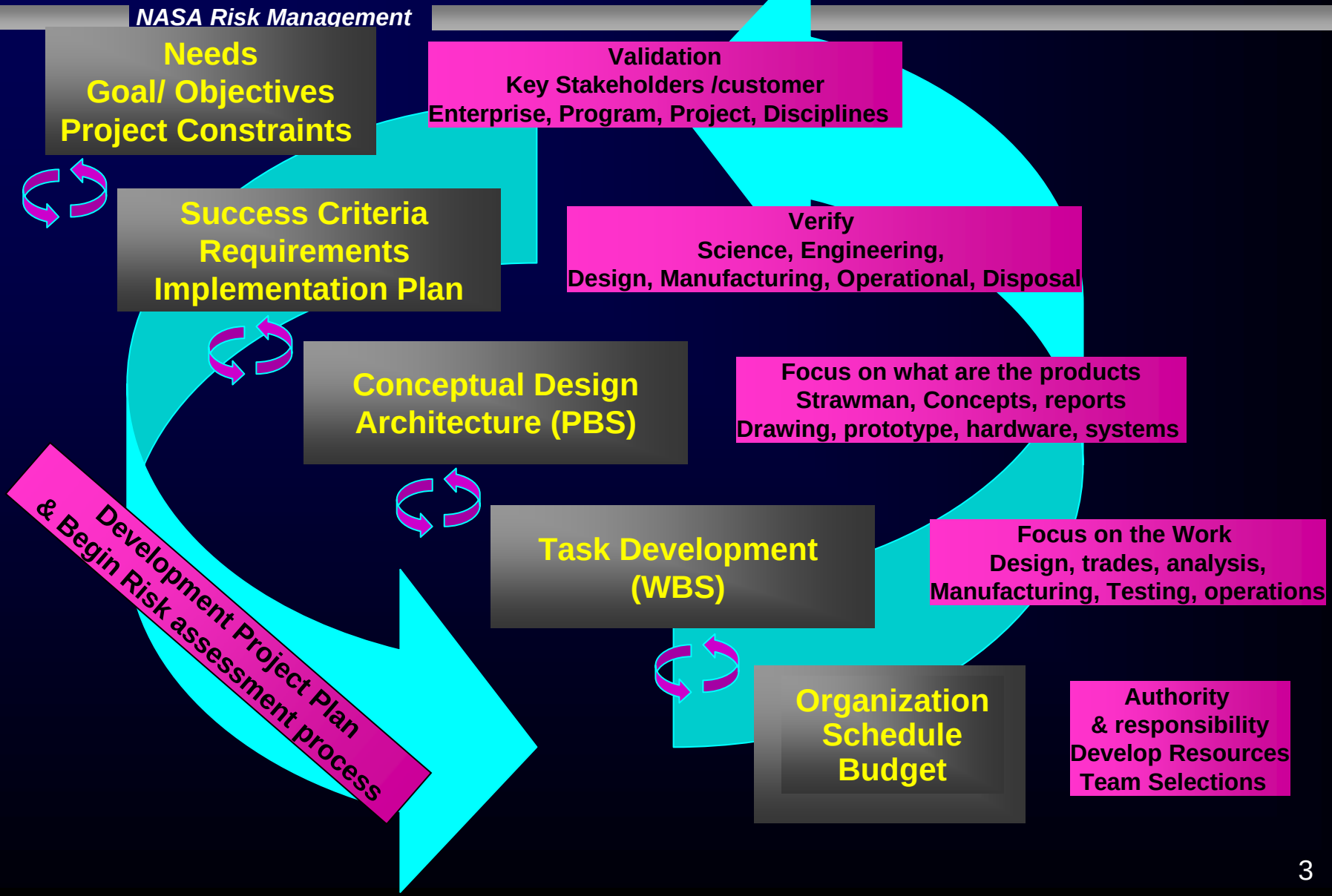
Continuous Risk Management at NASA
A Status Report

Risk Management Conference V
NASA Assurance Technology Center
October 27, 2004

Paradigm


Control
Identify
Analyze
Plan
Track
Communicate
Document

Project Planning Approach

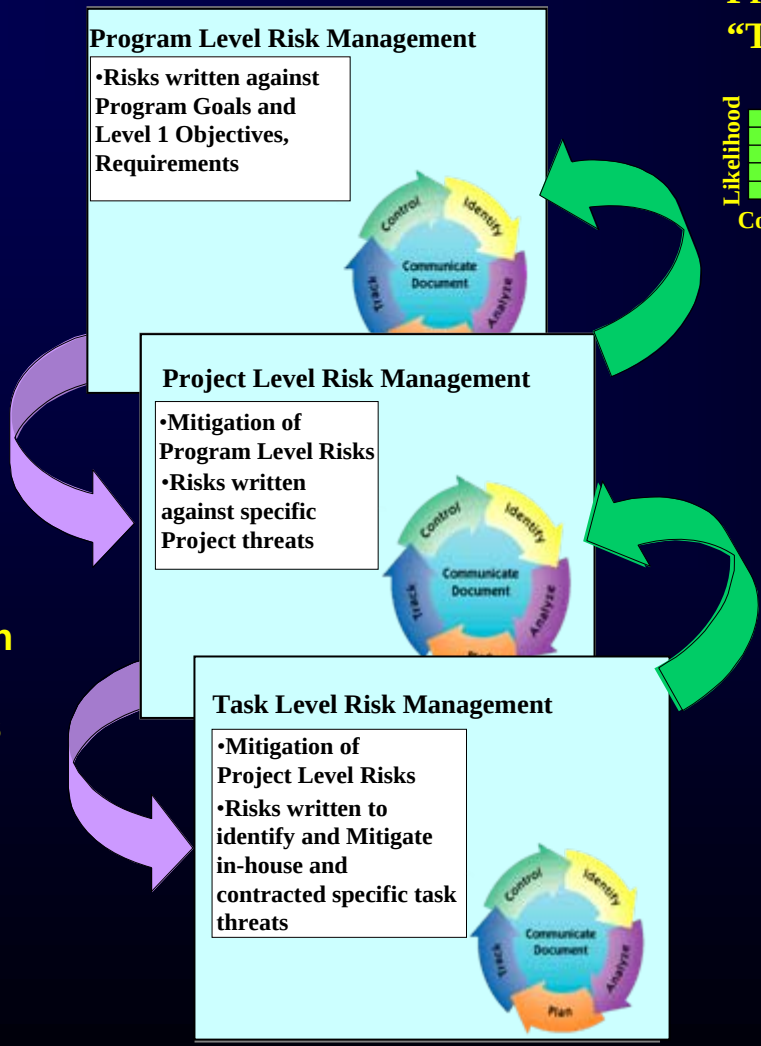


Requirement and Risk Flow

Requirements Flow-down

Program Goals, Objectives, Mission Success Criteria and Requirements

Project Goals, Objectives, Mission Success Criteria and Requirements



Program Level "Top N" Risks

Project Level "Top N" Risks

Project Level "Top N" Risks

Risk Reporting

Risk Identification

NASA Risk Management

Project Title:	**2.4 Integrated Tailored Aero Structures (ITAS)**
Objective:	**Develop ultralight smart materials and structures, aerodynamic concepts, and lightweight sub-systems to increase vehicle efficiency and maneuverability, leading to high altitude long endurance vehicles, planetary aircraft, advanced vertical and short takeoff and landing vehicles and beyond.**
Task Title:	**2.4.2 Actively Tailored High Lift Systems --- 2.4.2.1 High-Lift Concepts for ESTOL**
Objective/Milestone:	**Conduct Technology Demonstrations of High Lift Systems to a TRL Level of 5 within 5 years**

	Risk Statement			Before Mitigation					After Mitigation		
GAP / Issues / Problems / Concerns	**Condition** (Given that:)	**Consequence** (There is a possibility that:)	**Risk Priority**	**Likelihood**	**Impact**	**Timeframe (Immediate, Near, Long Term)**	**Mitigation**	**Mitigation Priority**	**Likelihood**	**Impact**	**Cost**
Identifying candidate technologies	There is a limited knowledge of, and access to, work being done or having been done for 20+ years, or to emerging new technologies	We will be unable to identify useful technologies that will achieve end goals		3	5	Immediate	Find experts	1	2	5	
							Establish search criteria	2			
							Perform Lit search	3			
							Conduct Workshops	4			
							Perform Trade studies	5			
Establishing decision criteria for down select	Limited specific requirements exist for downselect	We will select wrong technologies for further work that will not achieve our end goals		5	5	Immediate	Pushback on programs to define system requirements	1	4	5	
							Find experts	2			
							Establish selection process	3			
							Breakdown 15 year goals (5 years)	4	3	5	
							Engage external groups (think tanks)	5			
							Issue RFI	6			
							Constant iteration with other projects	7	2	5	
							Provide synergy among technology	8			
							Establish performance cutoff level	9			
							Conduct market study	10			
Finding Experts to evaluate candiate technologies											
Establish clear requirements for technology search criteria											
Getting a contract in place for identification process											
Access to past research/researchers with open mind											
Continuing resolutions limits availability of funding (budget stability)											

Purpose

Discuss risk management, program focus, and where we are going

Background

- Direct involvement by NASA Headquarters
- Enhance image
- Strong tie with Program/Project Management
  - Effective management of risks is integral to project management
- Update CRM Web site, tied in with APPL
- SMA support for all Center POCs
  - All Center SMA offices have reconfirmed or appointed POCs
- A consistent message to be presented across the Agency to all programs/projects
- Update standards, requirements, processes
- Transform CRM from a process based program to a decision based program

Roles

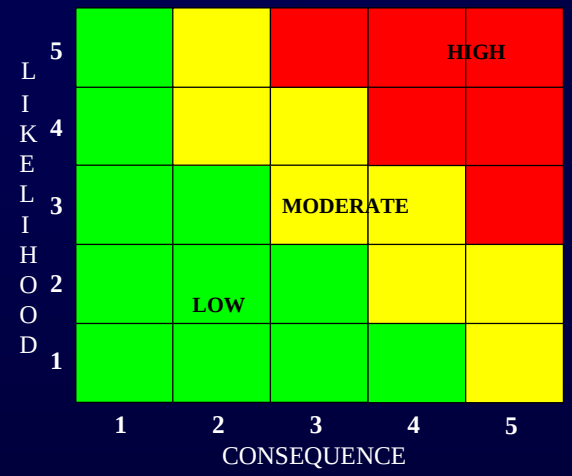
- Office of Safety and Mission Assurance
  - Keeper of the process
- Office of the Chief Engineer, 
  - Integrator with Project Management Training
- Mission Offices, programs, projects
  - Implementers of the process

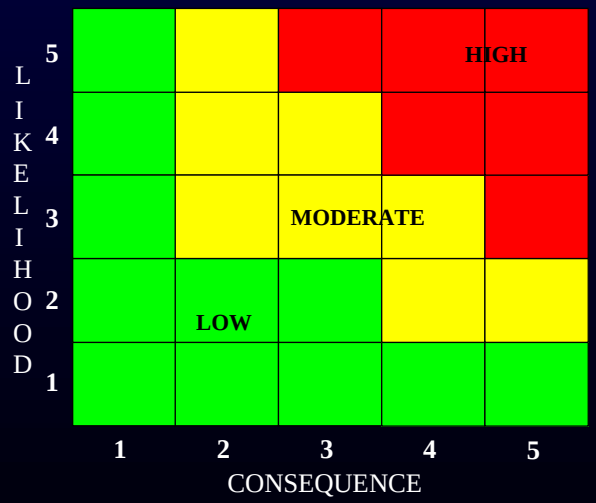
Program Focus

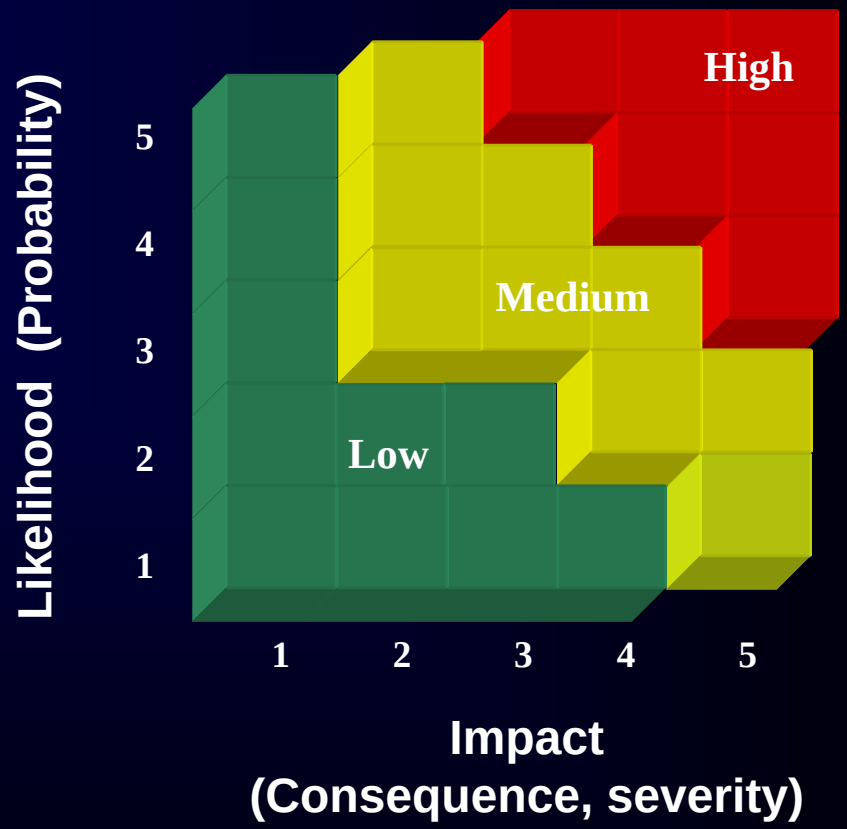
- Consistency
  - In implementation
  - In training/education
  - How we describe risks
- Risk based decisions
- Application & early identification of Risks by Program/Project
- Visibility

Consistency

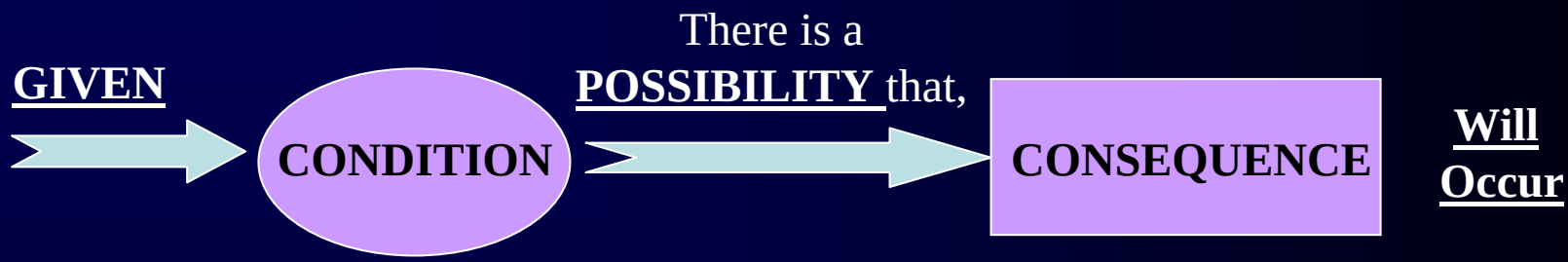
NASA Risk Management







Describing a Risk



For Example:

Condition
Given that the instrument / software interface requirements have 61 TBDs at contract award;

Consequence
There is a possibility that extensive cost overruns will be incurred in the performance of work by the software development contractor.

Consistency (con't)

- (Given that) The project was unable to verify the acceptability of the ADG201, linear CMOS High Speed Quad SPST Analog Switch due to a lack of radiation tolerance data; There is a possibility that the part may fail prematurely due to radiation exposure.

- (Given that) Unrealistic small business goals established for participation by subcontractors; Gov't rejects bids for not qualifying in the competitive range.

- Risk that 14x22 Wind Tunnel is not available.

Example - Risk Based Decisions

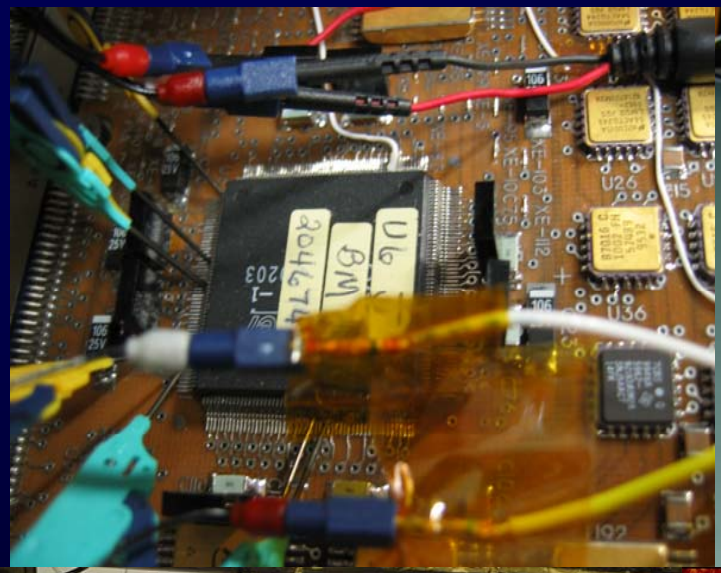
- Observatory has 2 science data processing boxes (Image Processors {IP})
  - 1 primary and 1 redundant
  - A potential flaw was identified

Given that Voltages at input pins of the IP FPGA devices exceed manufacturer's Absolute Max. voltage ratings;

There is a possibility that the IPs could fail on orbit resulting in instrument failure

- Failure condition in FPGAs was found to be industry wide, and several failures were identified by the Air Force and its prime contactors at the same time they were found by the project

FPGA in Image Processor



History of IP FPGA

- FPGA has experienced over a 1000 hours trouble free
  - It isn't know if the failure mechanisms is a cumulative or an infant mortality issue
- Launch is in 4 months
  - Special studies and research preliminary finding are not expected until 3 weeks after the schedule launch date
- Problem requires decisions and causes new risks

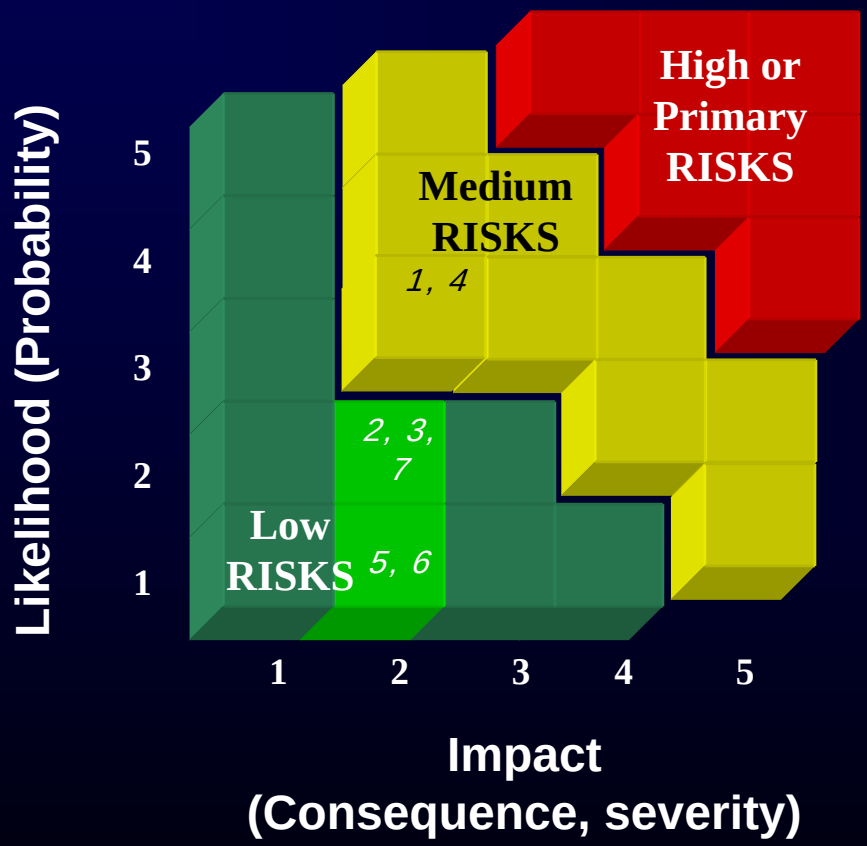
IPR Refurbishment- Probability Rating

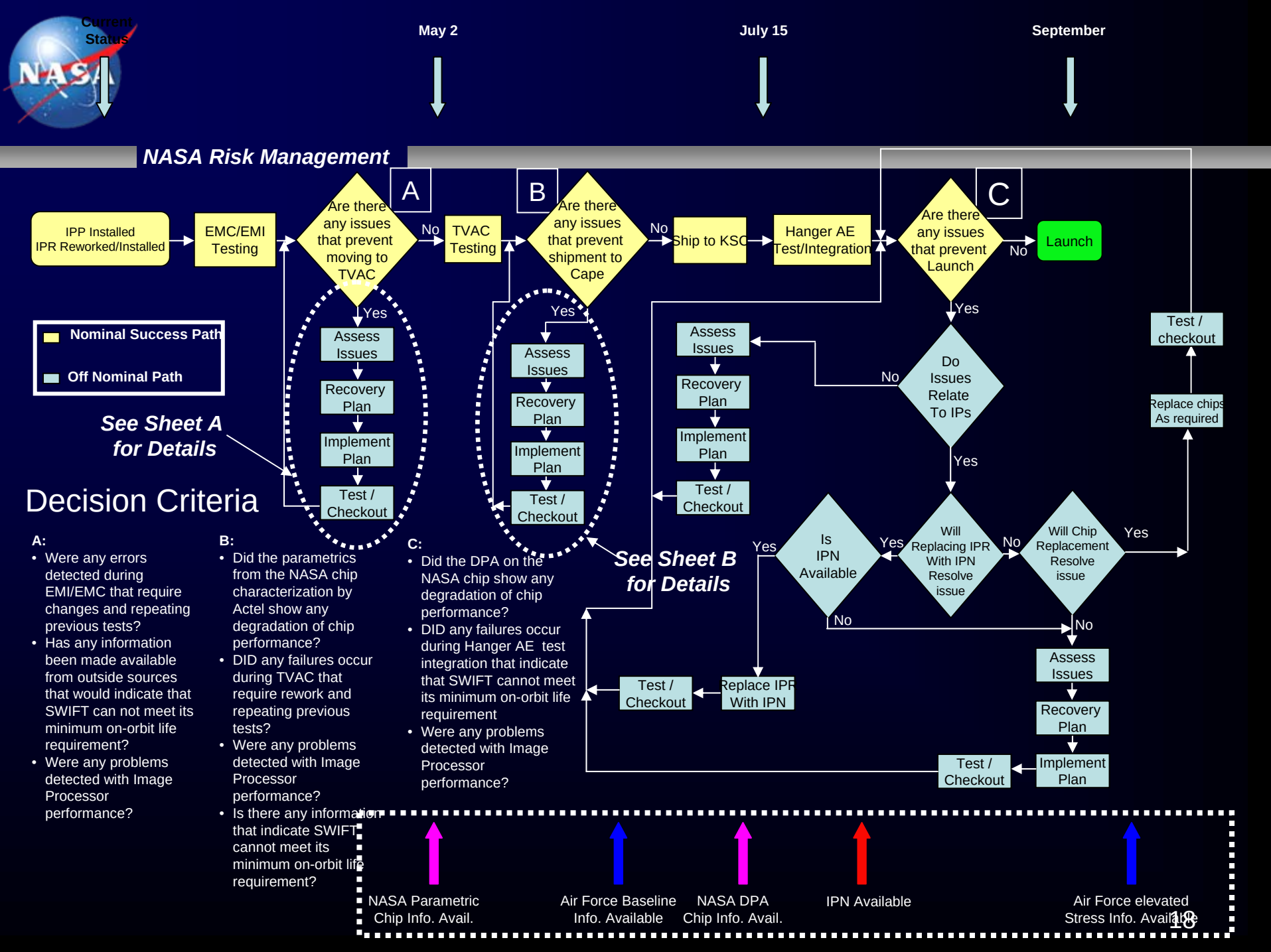
NASA Risk Management

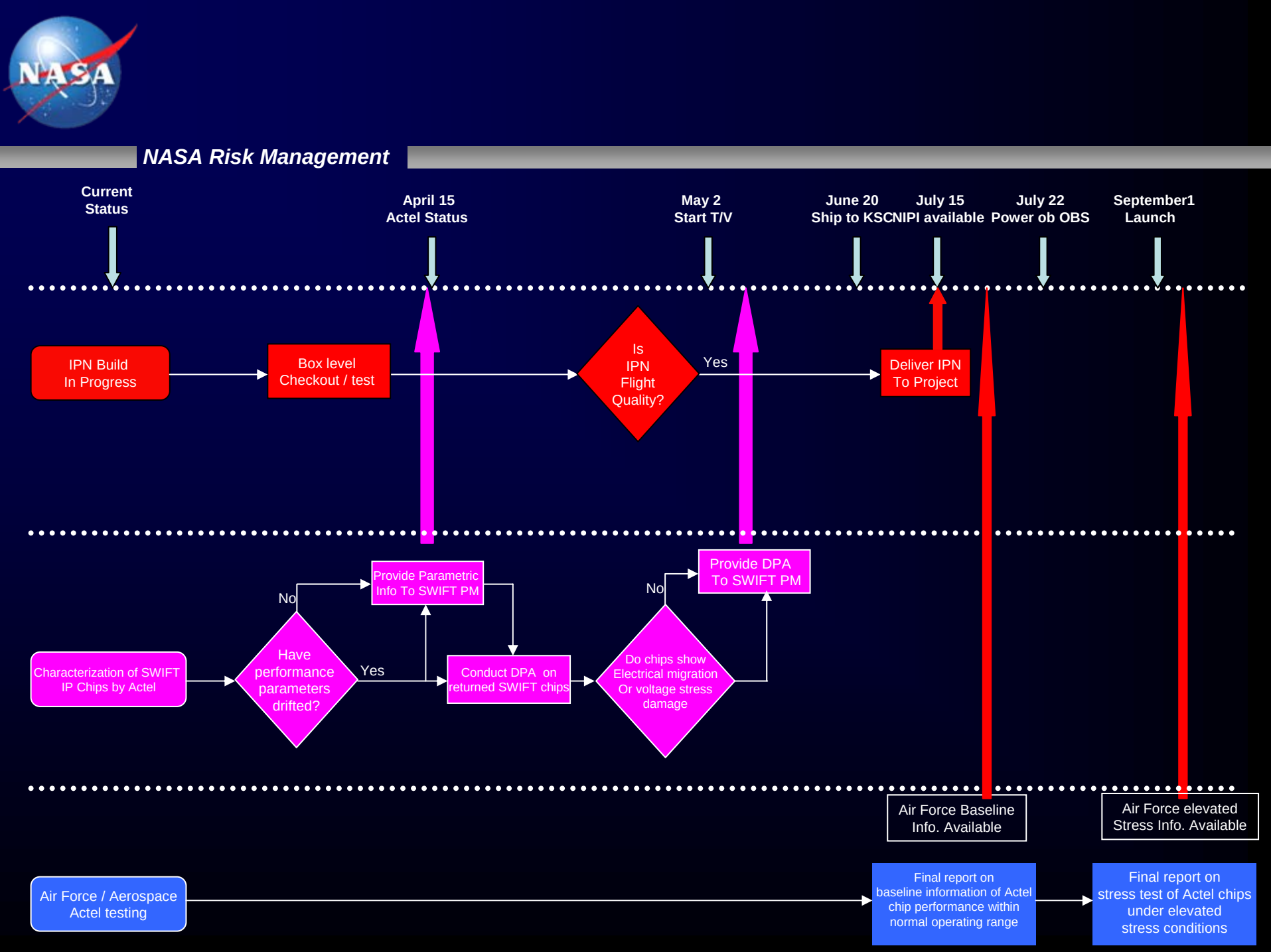
Item	Risk Area	Risk Type and Rationale	Level		Likelihood Description	Mitigation Cost	
						Hardware / Test	Time
1	IP Boards	**Workmanship:** a) 1 New PCB assembly, b) Two reworked PCB involving removal and replacement of 3 ACTELs (208 pins per ACTEL) per PCB.	3	Likely	Risk occurrence is likely, but workarounds may reduce the likelihood of risk occurrence.	480k	1 month
2	New Programming algorithm	New S/W released from ACTEL. Currently being characterized. Long terms effects are unknown.	2	Low Likelihood	Risk occurrence is a potential, but have usually mitigated this type of risk with minimal oversight and resources.	50k	2 months
3	EEE Parts	**Workmanship:** a) Risk of damage to parts during assembly process. b) ACTEL new programming algorithm side effects are unknown. c) Risk of infant mortality of new components. **d) Vcca electrical operating conditions still identical to present IPs.**	2	Low Likelihood	Risk occurrence is a potential, but have usually mitigated this type of risk with minimal oversight and resources.	Qual. Tests	3 months
4	IP BOX	**Workmanship:** Assembly errors experienced in the past despite written procedures.	3	Likely	Risk occurrence is likely, but workarounds may reduce the likelihood of risk occurrence.	Qual. Tests	3 months
5	IP Mechanical Stresses	Flight unit (Unit exposed to acceptance levels and durations)	1	Not Likely	Risk occurrence is very unlikely and should be effectively avoided based on standard practices.	500 k	1 week
6	Spacecraft	**Workmanship:** Team has experience performing this task.	1	Not Likely	Risk occurrence is very unlikely and should be effectively avoided based on standard practices.		2 weeks
7	"h" Harness	**Workmanship:** Damage to the harness has occurred during previous rework activities.	2	Low Likelihood	Risk occurrence is a potential, but have usually mitigated this type of risk with minimal oversight and resources.		2 weeks

Refurbishment Risk Analysis

IPR Refurbishment




Current Status
May 2
July 15
September
NASA Risk Management
IPP Installed
IPR Reworked/Installed
EMC/EMI Testing
A
Are there any issues that prevent moving to TVAC
No
TVAC Testing
B
Are there any issues that prevent shipment to Cape
No
Ship to KSC
Hanger AE Test/Integration
C
Are there any issues that prevent Launch
No
Launch
Yes
Assess Issues
Recovery Plan
Implement Plan
Test / Checkout
Nominal Success Path
Off Nominal Path
See Sheet A for Details
Decision Criteria
A:
Were any errors detected during EMI/EMC that require changes and repeating previous tests?
Has any information been made available from outside sources that would indicate that SWIFT can not meet its minimum on-orbit life requirement?
Were any problems detected with Image Processor performance?
B:
Did the parametrics from the NASA chip characterization by Actel show any degradation of chip performance?
DID any failures occur during TVAC that require rework and repeating previous tests?
Were any problems detected with Image Processor performance?
Is there any information that indicate SWIFT cannot meet its minimum on-orbit life requirement?
C:
Did the DPA on the NASA chip show any degradation of chip performance?
DID any failures occur during Hanger AE test integration that indicate that SWIFT cannot meet its minimum on-orbit life requirement
Were any problems detected with Image Processor performance?
See Sheet B for Details
Do Issues Relate To IPs
Is IPN Available
Will Replacing IPR With IPN Resolve issue
Will Chip Replacement Resolve issue
Replace IPR With IPN
Replace chips As required
Test / checkout
NASA Parametric Chip Info. Avail.
Air Force Baseline Info. Available
NASA DPA Chip Info. Avail.
IPN Available
Air Force elevated Stress Info. Available


NASA Risk Management
Current Status
April 15 Actel Status
May 2 Start T/V
June 20 Ship to KSC
July 15 NIPI available
July 22 Power ob OBS
September1 Launch
IPN Build In Progress
Box level Checkout / test
Is IPN Flight Quality?
Yes
Deliver IPN To Project
Provide Parametric Info To SWIFT PM
No
Have performance parameters drifted?
Yes
Characterization of SWIFT IP Chips by Actel
Conduct DPA on returned SWIFT chips
Do chips show Electrical migration Or voltage stress damage
No
Provide DPA To SWIFT PM
Air Force Baseline Info. Available
Air Force elevated Stress Info. Available
Air Force / Aerospace Actel testing
Final report on baseline information of Actel chip performance within normal operating range
Final report on stress test of Actel chips under elevated stress conditions

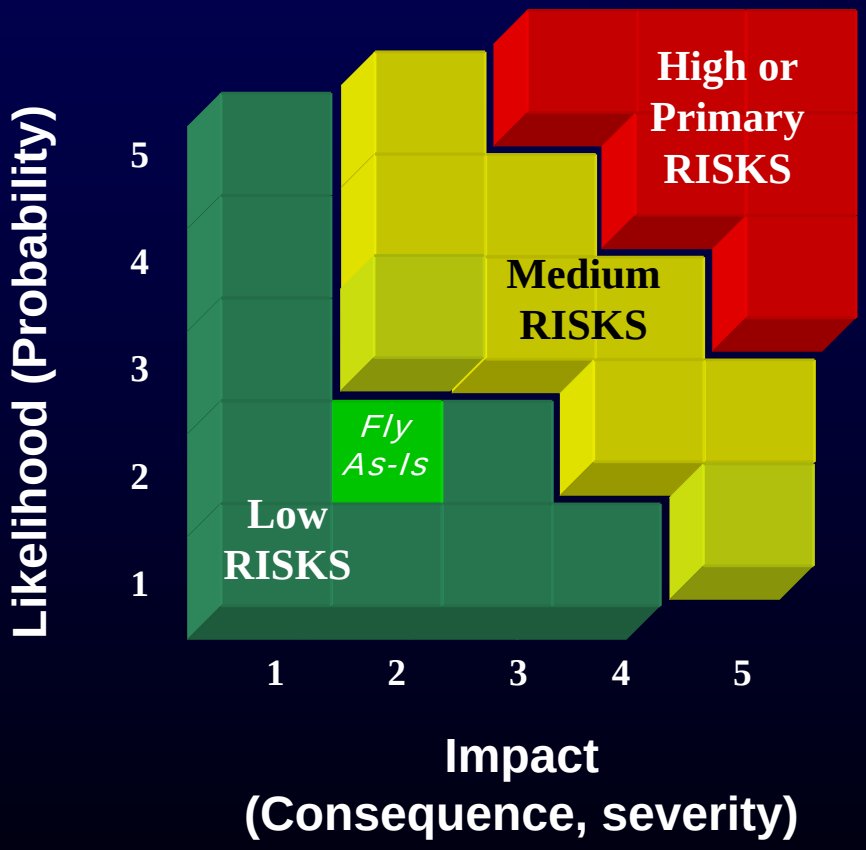
IP FPGA Probability Rating

Level	Likelihood Description		Rationale
5	Near Certainty	Risk occurrence is inevitable.	
4	Highly Likely	Risk occurrence is highly likely, but different approaches may reduce the likelihood of occurrence.	
3	Likely	Risk occurrence is likely, but workarounds may reduce the likelihood of risk occurrence.	
2	Low Likelihood	Risk occurrence is a potential, but have usually mitigated this type of risk with minimal oversight and resources.	**a)** Over ~1200 hrs of failure free operations (including environmental tests) for BOTH flight IPs. **b)** Failures reported in industry have manifested within the first ~160 hrs of operations. **c)** IP electrical environment different from industry reported failure environment. IP Vcca operating voltage 2.5 Vdc with very low occurrence spikes [>>3 sigma (voltage) and duty cycle <2E-7%] of less than 2 ns duration bringing the Vcca above 2.75 V but below 3V (2.75<Vcca<3.0)
1	Not Likely	Risk occurrence is very unlikely and should be effectively avoided based on standard practices.	

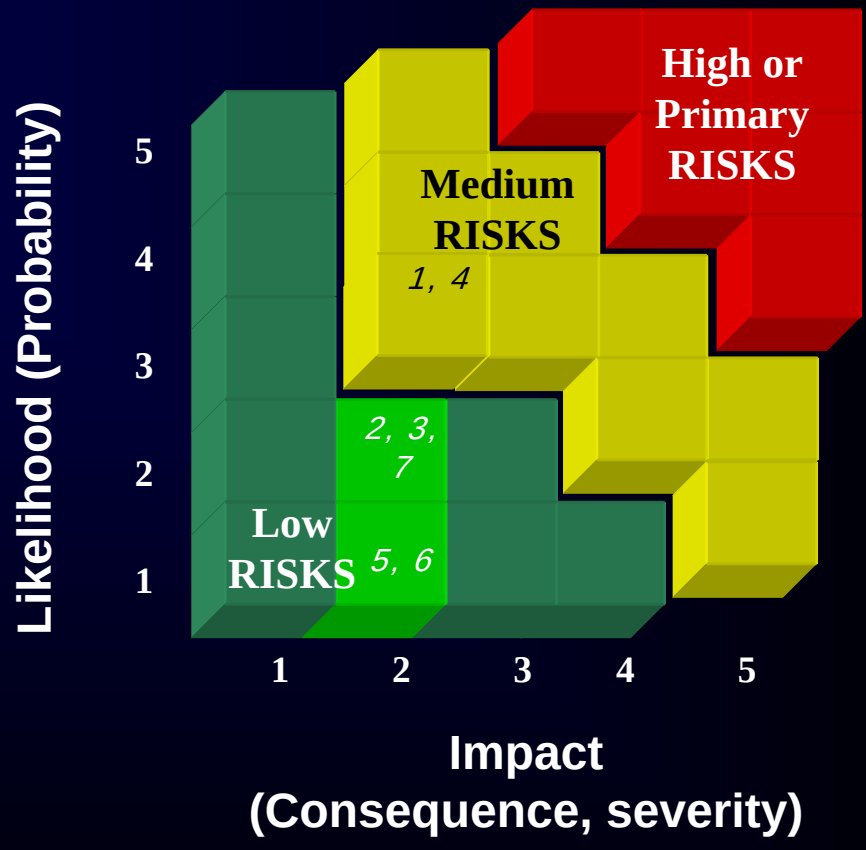
Impact on Technical Performance

Impact Rating	Technical/ Performance	BAT instrument configuration
5	Cannot meet minimum success criteria	
4	Major impact to full mission success	
3	Loss of system, With workarounds, moderate impact on full mission success	
2	Loss of redundancy or functional degradation, Minor impact to full mission success	**Fully redundant Image Processors**
1	Degradation of component, minor impact to full mission success	

Risk Decision



IPR Refurbishment



Example - Early Identification

- Problem/Needs
  - Potential for terrorist attacks against commercial airlines is still at a significantly high level.
  - Our approach to preventing another 9/11 is to have military fighter aircraft engage civil aircraft with the possibility of shooting them down.

- Project
  - Develop Technology that allows taking remote control of a civil airline and leading (flying) it away from populated areas to a remote safe location / landing site.

    (i.e. Develop a Tractor Beam)

What Decisions Would You Make?

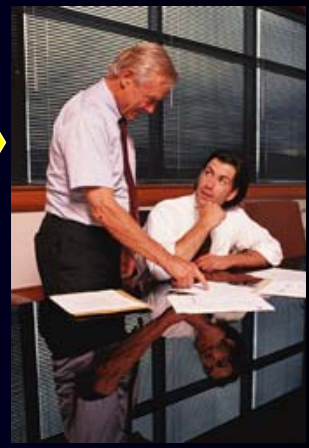
- What technology will be used?
- How will the technology be activated (what constitutes an alert)?
- How will alert be communicated?
- Who will respond (civilian or military)?
- Will response be airborne, ground based or space based?
- Will response sites be staffed 24/7?
- Where will landing site(s) be located?
- How many landing sites will there be?
- Who will be responsible for deployment of technology?
- Will technology be shared with other countries?
- What type of encryption be used?
- Will technology be adaptable to all aircraft?

- What are the risks involved in each of these decisions?

Visibility

Contractors vendors

Mission team

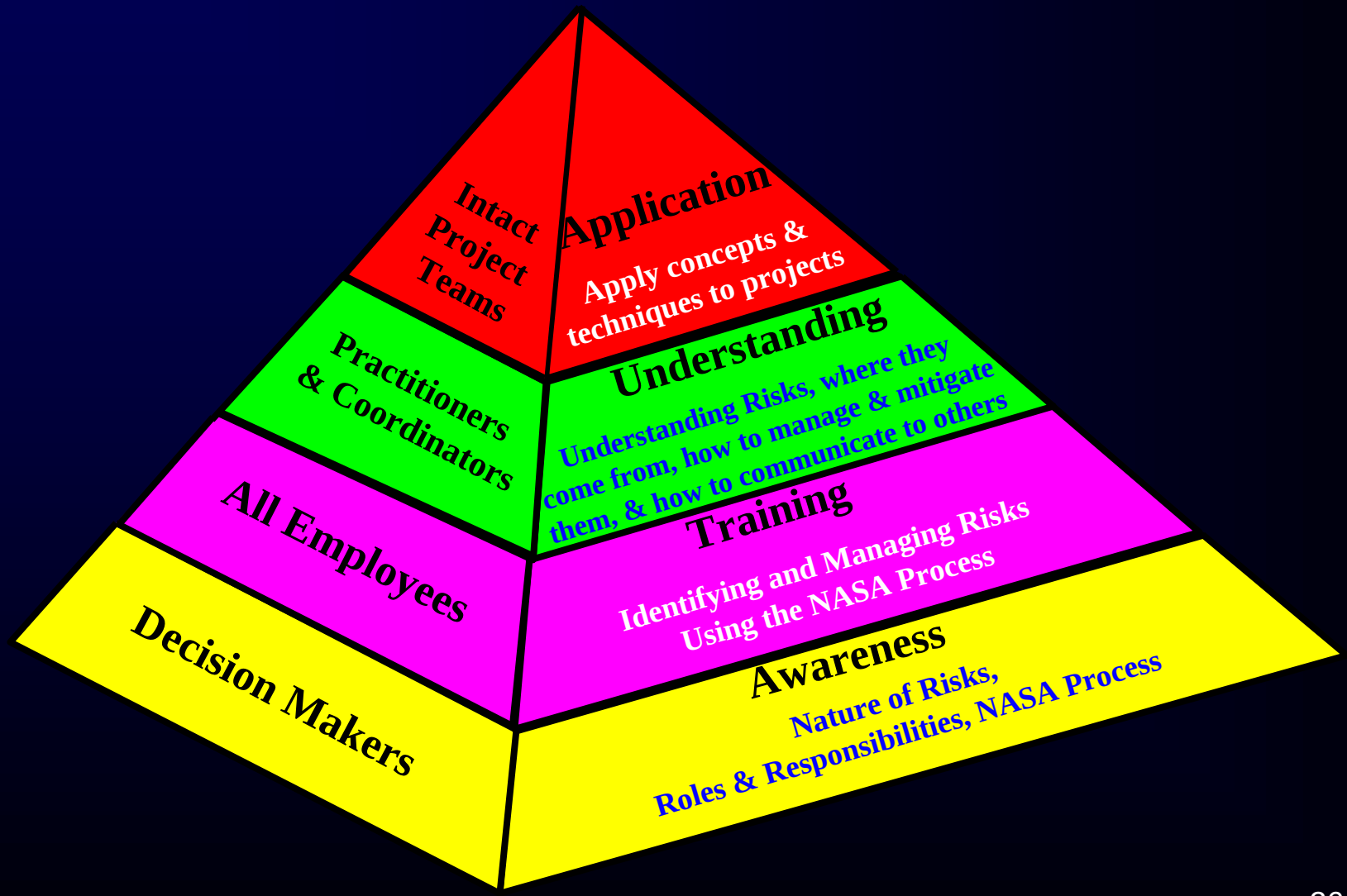


YOU!

Management team

Individual

NASA Risk Management Program



Program Scope

- Awareness Level
  - Briefings
- Training
  - Courses, Workshops
- Understanding
  - Courses, Workshops
- Application
  - Workshops, Professional Enhancement

Courses/Workshops

- Center/Headquarters Courses/Workshops
  - Foundations Course (6 hour)
  - Project Team Risk Management Course/Workshop (2 day)
  - Managing Flight Operations Risks Course (2 day)
  - Program/Project Briefing (4 hour)
  - Executive Overview Briefing (2 hour)
- APPL's Wallops Flight Facility Training Center
  - Risk Management for Practitioners (1 week)
  - Applied Project Management (1 week)
    - Focusing on identification and mitigation of risk

Risk Management for Practitioners

- Decisions – Uncertainty – Risk
  - Decision Example
- Concepts – Techniques – Principles
  - Foundations
- Methods – Tools – Techniques
  - Project Management, Requirements
  - Programmatic Tools
  - Safety, Reliability, Maintainability Tools
- Plans – Reporting – Presentations
  - Risk Reporting, Trending, Risk Management Plans

Safety, Reliability & Maintainability Tools

Safety and Security

- Preliminary Hazard Analysis
- System/Subsystem Hazard Analysis
- Fault Hazard Analysis
- FTA (Quantitative & Qualitative)
- Safety Requirements Compliance
- Orbital Debris Analysis
- Probabilistic Debris Impact Analysis
- Threat analysis, deterrents (Physical, IT)
- Intrusion / Penetration testing
- Injuries / Hazards / Emergency responses
- Detected intrusions (failed and successful)
- Center Network Environment blocks

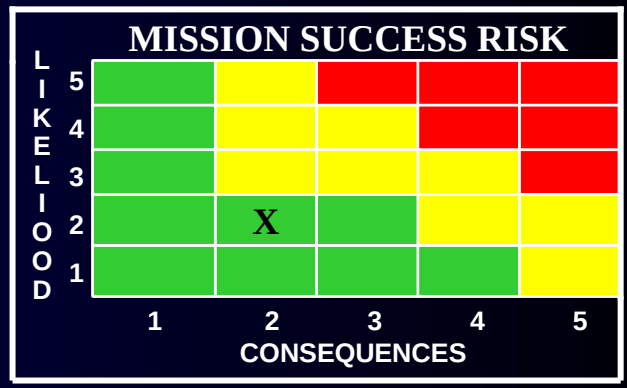
Technical Performance

- Verification & Validation
- Technology Maturity/ System complexity: Hardware / ops, Critical events or processes , Number of interfaces
- FTA, RBD, FMEA /FMECA, PRA
- Worse Case Analysis
- Limited Life Item Analysis
- Test Data/Trend Analysis
- Parts Stress and Derating Analysis Root Cause and Failure Analysis
- Software Reliability Analysis
- State-space Analysis (e.g., Markov Chains, Petri-nets)
- Maintainability Analysis/Testability Analysis
- Margins (Mass, Power, Data, Volume) FTA (Quantitative & Qualitative)
- Decision Tree/Event Tree/Event Sequence Diagrams
- Uncertainty Analysis/Sensitivity Analysis
- Probabilistic Risk Analysis

Example Reporting – FPGAs

NASA Risk Management

RISK TYPE: **Mission Success**
RISK CATEGORY: **Residual**
ORGANIZATION: **Program SMA**
ASSIGNED TO: **Risk Owner / GSFC**
INDEPENDENT ASSESSORS: **N/A**



RISK DESCRIPTION: (Condition)
Given that Voltages at input pins of the IP FPGA devices exceed manufacturer's Absolute Max. voltage ratings

RISK EFFECTS: (Consequence)
There is a possibility that the IPs could fail on orbit resulting in instrument failure

RISK REDUCTION ACTIONS:

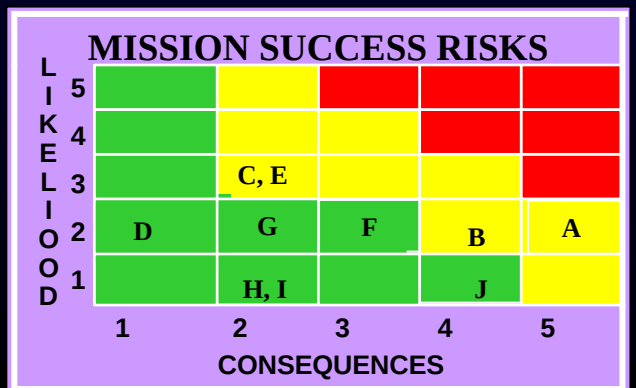
- Examination of test data showed that the absolute maximum voltage rating
- (AMR) on the part has not been exceeded.
- (Margin to AMR is 50mv.)
- Reliability analysis performed independently by Dr. Henning Leidecker/562 and Mr. Richard Katz/564, based on IP operating time combined with ACTEL testing failure rates, concluded that the probability of meeting the two year mission life is 92% to 98%.

CONSTRAINTS TO FLIGHT:
None

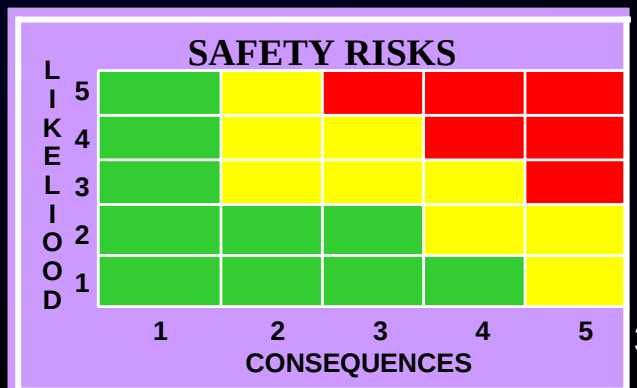
PROJECT POSITION:
Accept this risk / Residual

Risk Reporting Summary

NA = Not Applicable NR = Negligible Risk	Accountable Reviewing Organizations				
	Project	Project SMA	IIRT	IV & V	Minority Opinion
Assurance Elements					
A : Solar Array Mechanism Heritage	(1,5)	(2, 5)	(2,5)		
B : NFIs Limited Thermal Analysis	(1,4)	(2,4)	(2,4)		
C : FSW Sys level validation	NR	(2,4)	(2,4)		
D : Incomplete end-to-end Test of NFI	NR	(1,4)	(1,4)		
E : IIRT Key Management Practices	NA	NA	(3,2)		
F : Delay of Transition to Normal Operations	3,1	3,1	3,1		
G : Fault Protection Testing	(2,3)	(2,3)	(2,3)		
H : ADG201 – Radiation Tolerance	NR	(2,2)	(2,2)		
I : BAT IP Actel FPGAs	(2,2)	(2,2)	(2,2)		
J : BAT PCI Parity Error	(2,1)	(2,1)	(2,1)		



There are no known Safety Risks



Information Viscosity

- One of the 5 biggest challenges facing NASA is “Reducing the viscosity of Information” (How long does it take for information to flow through the organization.)

President – Disney Imagineering
Project Management Shared Experiences
Virginia Beach, VA